2\PRTS

[2345/165]

METHOD FOR GENERATING IDENTIFICATION NUMBERS

The present invention is directed to a method for generating a personal identification number (PIN), made up of a number of N decimal digits, to be used for money cards and other devices requiring security, from a binary number having L digits, in particular from a binary code specific to an individual.

When using automatic cash dispensers, such as ATM machines or similar devices where a plastic card is utilized, the user must often use a four-digit number (PIN) known only to himself in order to receive authorization. There are, by far, however, not as many different PINs as there are users, which is why each PIN exists many times over.

The PINs may only contain decimal digits, to enable them to be entered using numerical keypads. In addition, they are not supposed to begin with a zero. This means that, given four digit positions, the result is a range of 9000 different PINS. The theoretically lowest probability of correctly guessing a PIN is, thus, 1/9000.

The object of the present invention is to provide a method which will keep the probability of a PIN being correctly guessed as low as possible.

The realization underlying the present invention is that when the PINs are generated such that they are randomly uniformly distributed over the available number domain, the probability of a PIN being correctly ascertained becomes minimal. This is elucidated on the basis of the following example.

With the aid of an encryption algorithm, a secret key may be used to produce a binary code from personal data pertaining to the user. Using the DES or triple DES algorithm provided, for example, for generating PINs for money cards, a 64-digit binary code is generated from the data pertaining to one customer, with the assistance of a bank-specific key. From a 16-digit segment of this binary code, the PIN can be generated in the following manner, for example:

Four parts for each of the four digits of this binary number are combined into four decimal numbers. These four decimal numbers are divided by 10 (modulo function) to yield the four digits of the PIN as a remainder of a division. If the first digit is a zero, it is replaced by a one. To a large degree, however, the resultant PINs are unevenly distributed over the available number domain of 1 to 9000. If it begins with a 1, a PIN generated in this manner has a probability of being correctly guessed of even greater than 1/150.

If, on the other hand, one distributes the PINs uniformly over the number domain, then the rate of occurrence of each PIN is constantly 1/9000, and the probability of it being correctly guessed is, therefore, also minimal.

A first exemplary embodiment of the present invention provides for the first n1 digits of the binary number (B) to be converted in generally known fashion into a decimal number d1, the predefinable natural number n1 being selected so as to yield a natural number z1 such that the quotient $2^{n1}/(z1*9)$ is close to 1; and for the first decimal digit of the PIN to receive the value d1 modulo 9; for N-1 further groups of further n2 digits of the binary number (B) to be converted each time in generally known fashion into N-1 decimal numbers d2 through dN, the predefinable number n2 being selected so as to yield a natural number z2 such that the quotient $2^{n2}/(z2*10)$ is close to 1, the intention being to satisfy the condition: $0<=2^{n2}$ modulo $10<3$; and for the decimal digits 2 through N of the PIN to receive the values di modulo 10, i=2 through N.

To generate the first digit of the PIN, n1 is selected so that 2^{n1} is close to a multiple of 9. The n-1 digit part to the front of the binary number is interpreted as a decimal number. The integer remainder is calculated by dividing by 9. This remainder forms the first digit of the PIN. To generate digit 2 and the following digits of the PIN, n2 bits are split off each time. The number n2 is selected such that 2^n is close to a multiple of 10. The resulting number is interpreted as a decimal number. The integer remainder is calculated by dividing by 10. This remainder forms the respective digit of the PIN. It is true that no absolute uniform distribution is derived hereby. However, the greater n2 is, the more uniformly the PIN numbers are distributed.

For example, selecting n2=13 results in a number domain of from 1 to 2^{13}=8192. The digits 0, 1, 2 and 3 occur in the generated PINs with a probability of 820/8192, and the remaining digits with a probability of 819/8192. In particular, the method of the present invention avoids having the 1 occur all too often in the first digit position of the PIN.

A further exemplary embodiment of the present invention provides for nl and n2<=16 to be predefined.

Yet another exemplary embodiment of the present invention provides for N=4 to be selected.

Furthermore, it may be provided for the binary number (B) to have the length L=16, for N=4 to be predefined, and for nl=n2=4 to be predefined.

Yet another exemplary embodiment of the present invention provides for the binary number (B) to have the length L=3*n3, for n3 groups of three digits of the binary number (B) to be converted in generally known fashion into n3 decimal digits to generate the digits of the PIN, n3 being a natural number. In this variant, altogether 12 bits of the customer-specific binary code are used to generate the PIN. In each case, three bits of this binary number are interpreted as decimal digits between 1 and 8. The PINs produced in this manner are absolutely uniformly distributed.

Another possibility for generating absolutely uniformly distributed PINs within the particular number domain provides for the binary number to be completely converted into a decimal number, in order to generate the PIN in generally known fashion, and, if necessary, to add a correction value to the resultant decimal number such that the first digit of the decimal number becomes unequal to zero, the digits of the result forming the digits of the PIN.

To this end, it may be provided for the binary number to have a length L of 13, for the generated decimal number to have four digits, and for a preset value greater than 999 and smaller than 1807 to be added to the decimal number; for the binary number to have a length L of 16, for the generated decimal number to have five digit positions, and for a preset value greater than 9999 and smaller than 34465 to be added to the decimal number.

Furthermore, it may be provided in the first case (L=13) for the set of numbers 0 through 8191 to be allocated to n5 subsets Ml,...,Mn5, and for a preset value di to be added to the generated decimal number if it is an element of the set Mi, it holding that 999<dl<d2<...<dn5<1809, and n5 being a natural number.

Furthermore, it may be provided in the second case (L=16) for the set of numbers 0 through 65535 to be allocated to n5 subsets Ml,...,Mn5, and for a preset value di to be added to the generated decimal number if it is an element of the set Mi, it holding that 9999<dl<d2<...<dn5<34465, and n5 being a natural number.

Another exemplary embodiment of the present invention provides for executing the following steps to generate the first digits of the PIN:

- a pseudo-random number composed of up to 36 hexadecimal digits is generated from the binary number (B) of length L;
- each hexadecimal digit of this number is converted using one different one out of the 36 possible mathematical mappings of hexadecimal digits into the digits 1 through 9, into a digit of the digits 1 through 9;
- to even out the probability of the particular PIN digit occurring, the up to 36 decimal digits of the thus generated number are linked in a mathematical operation to form a decimal digit unequal to zero, which represents the first digit of the PIN;

and for the following steps to be executed for the second and each following digit of the PIN to be generated:

- a pseudo-random number composed of up to 210 hexadecimal digits is generated from the binary number (B) of length L;
- each hexadecimal digit of this number is converted into one decimal digit using each time one different one out of the 210 possible mathematical mappings of hexadecimal digits into decimal digits;
- to average out the probability of the particular PIN digit occurring, the up to 210 decimal digits of the thus generated number are linked in a mathematical operation to form a decimal digit, which represents the particular digit of the PIN;

For this purpose, it may be provided that the first digit of the PIN is generated in that the up to 36 digits are linked using the group operation of any arbitrary mathematical group of the order 9, and that the second and the following digits of the PIN are generated, in that the up to 210 digits are linked using the group operation of any arbitrary mathematical group of the order 10.

In this exemplary embodiment of the method of the present invention, one hexidecimal number each is generated from N groups of 4 bit length each. It is intended at this point to convert it into a decimal digit. Altogether (10 over 6) = (10 over 4) = 210 different mappings of the hexadecimal digits into the set of decimal digits are available for this conversion. One possible mapping is forming the remainder in a division by 10: (0 -> 0, 1 -> 1, 2 -> 2, 3 -> 3, 4 -> 4, 5 -> 5, 6 -> 6, 7 -> 7, 8 -> 8, 9 -> 9, A -> 0, B -> 1, C -> 2, D -> 3, E -> 4, F -> 5). Following this mapping operation, the digits 0 to 5 occur with the rate of occurrence of 1/8, and the digits from 6 to 9 with the rate of occurrence of 1/16. At this point, in order to obtain digits whose probability of occurrence does not deviate or deviates imperceptibly from 1/10, it is proposed to convert the 210 hexadecimal digits, which were generated, for example, by applying the above-mentioned DES algorithm 14 times to the 64-digit binary initial number, (therefore, pseudo-random number, since the generated number is in no way randomly formed), using one each of the other 210 possible mappings, into a decimal digit and, subsequently, linking all 210 decimal digits to one single digit using a group operation of a mathematical group having ten elements. The probability of occurrence of each of the thus generated decimal digits is close to 1/10.

A next exemplary embodiment of the present invention provides for the additive group of the integers modulo 10 to be used to link the up to 210 digits. In this context, 210 decimal digits are linked to form one single digit, in that one adds all digits and takes as a result, the remainder of a division of the sum by 10. The ten possible results that occur in the process constitute the elements of the additive group $Z_{10,+}$.

Another exemplary embodiment of the present invention provides for using the multiplicative group of the integers modulo 11 for linking the up to 210 digits. This group Z^*_{11} likewise has ten elements and is, therefore, suited for linking the numbers to a decimal digit. In Z^*_{11}, one calculates by multiplying two elements and dividing the result by 11. The remaining remainder forms the result of the operation. The zero is removed from the group. The 0 occurring in the digits indexes element no. 10 of the group Z^*_{11}.

Another exemplary embodiment of the present invention provides that the group of the symmetric mappings of a regular pentagon (dihedral group) be used for linking the up to 210 digits, each of the ten symmetric mappings of this group being assigned a different decimal digit. To this end, it may also be provided for the digit 0 to be assigned to the identity mapping, digits 1 through 4 to be assigned the four rotations about the midpoint of the pentagon, digits 5 through 9 to be assigned to the five reflections about the five axes of symmetry of the pentagon. If one executes two symmetric mappings one after another, then a symmetric mapping again results. Based on these allocations, one can set up the following multiplication table:

*	0	1	2	3	4	5	6	7	8	9
0	0	1	2	3	4	5	6	7	8	9
1	1	2	3	4	0	6	7	8	9	5
2	2	3	4	0	1	7	8	9	5	6
3	3	4	0	1	2	8	9	5	6	7
4	4	0	1	2	3	9	5	6	7	8
5	5	9	8	7	6	0	4	3	2	1
6	6	5	9	8	7	1	0	4	3	2
7	7	6	5	9	8	2	1	0	4	3
8	8	7	6	5	9	3	2	1	0	4
9	9	8	7	6	5	4	3	2	1	0.

With the assistance of this table, the 210 digits are linked to one single digit in that, utilizing the result from the previous operation as a row indicator and utilizing the next digit as a column indicator, the next result in the table is read off successively until all digits are considered. The last result forms the desired digit of the PIN.

Exemplary embodiments of the present invention are represented by several figures in the drawing and are elucidated in the following description. The figures show:

Figure 1 a diagram for generating a customer-specific binary code;

Figure 2 a diagram for generating a PIN through conversion to a decimal number;

Figure 3 a diagram for generating a PIN by a digit-by-digit conversion into decimal numbers;

Figure 4 a diagram for generating a PIN by a digit-by-digit conversion, including modulus formation; and

Figure 5 a diagram for generating a PIN by reducing hexadecimal numbers with the assistance of mathematical groups.

Identical or corresponding parts are provided with the same reference numerals in the figures.

Figure 1 depicts a flow diagram for converting personal data Dc of a customer using a secret key K into a binary number B of L bits length. The binary number B is part of the 64-bit long encryption result, which was generated from the customer data Dc using the DES algorithm.

If the length of the binary number B equals 13, and if the number of the PIN digits to be generated equals 4, then the PIN, as shown in Figure 2, can be generated by interpreting the binary number B as decimal number D by adding a constant C thereto. The constant is to be selected such that the PIN does not have any leading zeros. In this manner, 8192 different PINS can be generated, which are absolutely uniformly distributed over the number domain in question.

Figure 3 depicts how a binary number of length 13 can be converted into a PIN in that for each digit of the PIN to be generated, a number of bits of the binary number is converted into a decimal number, and a constant C is added to the resultant number D, to avoid having leading zeros of the PIN.

In this manner, 7777 different PINS may be generated, which are absolutely uniformly distributed over the number domain in question.

Another possibility for generating nearly equally distributed PINs from a binary number B is illustrated in Figure 4. The binary number B has 52 digit positions. To generate the four-digit PIN, the binary number B is subdivided into four subsets, which, in the example, have the same length. Each of these subsets is interpreted as a decimal number. The first digit of the PIN is derived as a remainder of a division of the first decimal number by 9. The following digits of the PIN are derived in each case as a remainder of a division of the following decimal number by 10. In this manner, 9000 different PINS may be generated, which are absolutely uniformly distributed.

From the personal data Dc of a customer, as shown in Figure 5, a sequence of 210 hexadecimal digits is generated with the assistance of a secret key and a random-number generator, in that, for example, an encryption result of the DES algorithm from Figure 1 is again encrypted using the algorithm, and so forth. The 14 64-digit binary codes resulting therefrom are converted into 14 hexadecimal numbers Hi, each having 16 digits. Lined up, this yields 224 hexadecimal digits, of which 210 enter into the generation of the PIN.

There are 210 different possibilities fi for mapping the set of 16 hexadecimal digits into the set of the 10 decimal digits. Therefore, each of the 210 hexadecimal digits is converted using a different one of these mappings into a decimal digit di. In order to produce a digit Zi of a PIN from the 210 decimal digits, they are successively linked using the group operation F of any arbitrary ten-element mathematical group; the last result is the sought after digit. Thus, the previously non-uniform, statistical distribution of the 210 decimal digits is evened out. The entire process is repeated for each of the digit positions Z2 through Z4 of the PIN.

Analogously for the first digit of the PIN, 36 hexadecimal digits are generated, which are mapped with every other one of the 36 possible mappings of the hexadecimal digits into the set of the digits 1 through 9, into a digit between 1 and 9. The 36 decimal digits are linked to the first digit of the PIN using the group operation of any arbitrary mathematical group of the order 9. This enables 9000 different PINs to be generated which are nearly uniformly distributed. In generating 10^5 PINs, the maximum non-uniformities amounted to about 1.5 percent. This does not significantly raise the probability of a PIN being accidentally correctly guessed as compared to the theoretical minimum value. Thus, the method functions very reliably.

All mathematical groups having ten elements are fundamentally suited for use with this method. Known representatives include the additive group of the integers modulo 10, $Z_{10,+}$, the multiplicative group of the integers modulo 11, Z^*_{11} , as well as the group of the symmetric mappings of a regular pentagon D5, the so-called dihedral group. In the last instance, one decimal digit, which may be used for the calculation, is assigned to each of the individual elements of the group.